



TITLE:

楕円曲線のHasse不変量について (代数的整数論と数論的幾何学)

AUTHOR(S):

石橋, 睦; 佐藤, 尚宜; 白谷, 克巳

CITATION:

石橋, 睦 ...[et al]. 楕円曲線のHasse不変量について(代数的整数論と数論的幾何学). 数理解析研究所講究録 1995, 925: 110-116

ISSUE DATE:

1995-10

URL:

<http://hdl.handle.net/2433/59802>

RIGHT:

楕円曲線の Hasse 不変量について

鹿児島工業高専 石橋 睦 (Makoto ISHIBASHI)
九大 数理学研究科 佐藤尚宜 (Hisayoshi SATO)
九大 数理学研究科 白谷克巳 (Katsumi SHIRATANI)

§1. 序

標数 $p \geq 5$ の素体 $\mathbf{GF}(p)$ 上に定義された楕円曲線 $E_{a,b}: y^2 = x^3 + ax + b$ を考える. 定義方程式の右辺の $\frac{p-1}{2}$ 乗 $(x^3 + ax + b)^{\frac{p-1}{2}}$ における x^{p-1} の係数 $H_{a,b}$ を Hasse 不変量という. Hasse 不変量は $E_{a,b}$ の関数体の p 次不分岐拡大の存在に深く関係している. $H_{a,b}$ に対する公式ははじめ Deuring[2] によって計算された. 最近になって Kaneko[4] によってある超幾何多項式を用いて計算されている. また Koike[7] は有限体上の超幾何級数を用いて Legendre form で与えられた楕円曲線などの Frobenius 自己同型の trace を表示している. 一方 Chowla-Dwork-Evans[1] は楕円曲線 $y^2 = x^3 + x$ の Hasse 不変量に関係した 2 項係数に対する p を法とする公式を与えている.

ここではまず楕円曲線 $y^2 = x^3 + 1$ の Hasse 不変量に関係した 2 項係数の p の高いべきを法としたときの公式を与え, 次に一般の $E_{a,b}$ に対する Hasse 不変量の有限体上での超幾何級数を用いる簡明な表示を得る.

§2. $y^2 = x^3 + 1$ に関係した 2 項係数に対する合同式

素数 p を $p \equiv 1 \pmod{3}$ とし 楕円曲線 $y^2 = x^3 + 1/\mathbf{GF}(p)$ をとる. $\mathbf{GF}(p)$ と $\mathbf{Z}/p\mathbf{Z}$ を同一視する. このとき この楕円曲線の Hasse 不変量は $\text{mod } p$ で $\left(\frac{p-1}{3}\right)$ に等しい. ω を $\mathbf{GF}(p)$ の Teichmüller 指標 とし Koike[6] によって定義された有限体上の 2 項係数

$$\left(\frac{\omega^i}{\omega^k}\right)^* = \frac{\omega^k(-1)}{p-1} J(\omega^i, \omega^{-k}) = \frac{1}{1-p} \frac{\Gamma_p\left(\frac{i-k}{p-1}\right) \Gamma_p\left(\frac{k}{p-1}\right)}{\Gamma_p\left(\frac{i}{p-1}\right)}, \quad 0 \leq k \leq i$$

を考える. ただし $J(\omega^i, \omega^{-k})$ は Jacobi 和, Γ_p は p 進 gamma 関数, また二番目の等式は Gross-Koblitz の公式による.

$i = \frac{p-1}{2}, k = \frac{p-1}{3}$ とし Γ_p の関数等式, Taylor 展開, 及び Diamond の公式を用いると任意の自然数 f に対して

$$\left(\omega^{\frac{p-1}{2}}\right)^* \equiv \frac{-1}{p-1} \left(\frac{p^f-1}{2}\right) \left(\frac{p^{f-1}-1}{3}\right)^{-1} \left(1 + \frac{2}{3}(2^{p^{f-1}(p-1)} - 1) - \frac{3}{4}(3^{p^{f-1}(p-1)} - 1)\right) \pmod{p^{2f}} \quad (1)$$

を得る. 更に $\left(\omega^{\frac{p-1}{2}}\right)^*$ を $\mathbf{Q}(\sqrt{-3})$ において

$$\left(\omega^{\frac{p-1}{2}}\right)^* = \frac{(-1)^{\frac{p-1}{6}}}{p-1} B, \quad B = p^{-1} g(\omega^{\frac{p-1}{2}}) g(\omega^{\frac{2(p-1)}{3}}) g(\omega^{\frac{5(p-1)}{6}}),$$

$g(\omega^a) : \text{Gauss 和}$

と表すことができ B は $\mathbf{Q}(\sqrt{-3})$ の整数となる. そこで

$$B = \alpha + \beta w, \quad w = \frac{1 + \sqrt{-3}}{2}, \quad \alpha, \beta \in \mathbf{Z}$$

とおく. このとき

$$N_{\mathbf{Q}(\sqrt{-3})/\mathbf{Q}}(B) = p = \alpha^2 + \alpha\beta + \beta^2$$

であるが, この p の分解における α, β の満たす条件を有理的に表す. 実際 ζ を 1 の原始 3 乗根として, $k \in \{1, -1, \zeta, -\zeta, \zeta^2, -\zeta^2\}$ に対して

$$\eta_k = \sum_{\substack{1 \leq x \leq p-1 \\ \omega^{\frac{p-1}{6}}(x) = k}} \zeta_p^x, \quad (\zeta_p : 1 \text{ の原始 } p \text{ 乗根})$$

と置くと, Gauss 和の定義により

$$\begin{aligned} g(\omega^{\frac{2(p-1)}{3}}) &\equiv \eta_1 + \eta_{-1} + \eta_\zeta + \eta_{-\zeta} + \eta_{\zeta^2} + \eta_{-\zeta^2} \equiv -1 \pmod{\mathfrak{l}_3}, \\ g(\omega^{\frac{p-1}{2}}) &\equiv g(\omega^{\frac{5(p-1)}{6}}) \equiv \eta_1 - \eta_{-1} + \eta_\zeta - \eta_{-\zeta} + \eta_{\zeta^2} - \eta_{-\zeta^2} \pmod{\mathfrak{l}_3} \end{aligned}$$

となる. ここで イデアル $\mathfrak{l}_3 = (\sqrt{-3})$ である. 故に

$$\begin{aligned} pB &= p\alpha + p\beta w \\ &\equiv -g(\omega^{\frac{p-1}{2}})^2 \equiv (-1)^{\frac{p-1}{2}+1} \pmod{\mathfrak{l}_3}. \end{aligned}$$

従って

$$\alpha - \beta \equiv (-1)^{\frac{p+1}{2}} \pmod{3} \quad (2)$$

である.

一方, pB を $\mathbf{Q}(\zeta, \zeta_p)$ の元として表すと

$$\begin{aligned} pB &= g(\omega^{\frac{p-1}{2}}) \{ (\eta_A \eta_C - \eta_B \eta_D) + (\eta_A \eta_D + \eta_B \eta_C - \eta_B \eta_D) \zeta \} \\ &= p(\alpha + \beta) + p\beta\zeta. \end{aligned}$$

ただし

$$\begin{aligned} \eta_A &= \eta_1 + \eta_{-1} - \eta_{\zeta^2} - \eta_{-\zeta^2}, & \eta_B &= \eta_{\zeta} + \eta_{-\zeta} - \eta_{\zeta^2} - \eta_{-\zeta^2}, \\ \eta_C &= \eta_1 - \eta_{-1} - \eta_{\zeta} + \eta_{-\zeta}, & \eta_D &= \eta_{\zeta^2} - \eta_{-\zeta^2} - \eta_{\zeta} + \eta_{-\zeta} \end{aligned}$$

となる. 故に $1, \zeta$ が $\mathbf{Q}(\zeta_p)$ 上の $\mathbf{Q}(\zeta, \zeta_p)$ の底であることより

$$\beta \equiv 0 \pmod{2} \quad (3)$$

(従って $\alpha \equiv 1 \pmod{2}$) である. $\mathbf{Q}(\sqrt{-3})$ の単数の個数は 6 で, $p = N(\epsilon(\alpha + \beta w))$ (ϵ : 単数) なる分解も 6 通り考えられるが (2), (3) を満たすものはひとつしかなく 従って p の分解が確定する.

さて B の \mathbf{C}_p への埋め込みは $B\bar{B} = p$ であることから Gross-Koblitz 公式を用いれば $B_0 = \Gamma_p(\frac{1}{2})\Gamma_p(\frac{1}{3})\Gamma_p(\frac{1}{6})$, p/B_0 の二つであることがわかる. $B_0 + p/B_0 = 2\alpha + \beta$ だから

$$B_0 \equiv (2\alpha + \beta) + \frac{1}{2} \sum_{k=1}^{2f-1} \binom{\frac{1}{2}}{k} (-1)^k \frac{4^k}{(2\alpha + \beta)^{2k-1}} p^k \pmod{p^{2f}}$$

となる. よって B の埋め込みを B_0 にすれば $u = 2\alpha + \beta$ とおいて (1) とともに次を得る.

定理 1. p を $p \equiv 1 \pmod{3}$ なる素数とし, $4p = u^2 + 3v^2$, $u, v \in \mathbf{Z}$ を $u \equiv (-1)^{\frac{p-1}{2}} \pmod{3}$, $v \equiv 0 \pmod{2}$ と p を分解するとき

$$\begin{aligned} \left(\frac{\frac{p^f-1}{2}}{\frac{p^f-1}{3}} \right) \left(\frac{\frac{p^{f-1}-1}{2}}{\frac{p^{f-1}-1}{3}} \right)^{-1} &\equiv (-1)^{\frac{p+1}{2}} \left\{ u + \frac{1}{2} \sum_{k=1}^{2f-1} \binom{\frac{1}{2}}{k} (-1)^k \frac{4^k}{u^{2k-1}} p^k \right\} \\ &\quad \cdot \left\{ 1 - \frac{2}{3}(2^{p^{f-1}(p-1)} - 1) + \frac{3}{4}(3^{p^{f-1}(p-1)} - 1) \right\} \pmod{p^{2f}}. \end{aligned}$$

特に $f = 1$ のとき

$$\left(\frac{\frac{p-1}{2}}{\frac{p-1}{3}} \right) \equiv (-1)^{\frac{p+1}{2}} \left(u - \frac{p}{u} \right) \left(1 - \frac{2}{3}(2^{p-1} - 1) + \frac{3}{4}(3^{p-1} - 1) \right) \pmod{p^2}.$$

§3. 有限体上の超幾何級数と Hasse 不変量

$\mathbf{GF}(p)$ ($p \geq 5$) 上の楕円曲線 $E_{a,b}: y^2 = x^3 + ax + b$ の Hasse 不変量を計算する. 以下 $\mathbf{GF}(p)$ と $\mathbf{Z} \bmod p$ を同一視する. $H_{a,b}$ の定義により

$$\begin{aligned} H_{a,b} &= (1 + ax^{-2} + bx^{-3})^{\frac{p-1}{2}} \text{ における } x^{-\frac{p-1}{2}} \text{ の係数} \\ &= \sum_{3i+2k=\frac{p-1}{2}} \frac{\left(\frac{p-1}{2}\right)!}{i!k!\left(\frac{p-1}{2}-i-k\right)!} a^k b^i \end{aligned}$$

となる. この和を Γ_p を用いて変形するが, p を 12 を法にして場合に分ける.

例えば $p \equiv 5 \pmod{12}$ で $a \neq 0$ のとき, $i = 2i_0$, $k = 3k_0 + 1$ とおくと

$$\begin{aligned} i! &= 2^{2i_0} i_0! \left(\frac{1}{2}\right)_{i_0}, \\ k! &= \{(-3)^{3i_0} \left(\frac{1-p}{12}\right)_{i_0} \left(\frac{5-p}{12}\right)_{i_0} \left(\frac{9-p}{12}\right)_{i_0} \Gamma_p\left(\frac{1-p}{4}\right)\}^{-1}, \\ \left(\frac{p-1}{2} - i - k\right)! &= \left(\frac{p+3}{4}\right)_{i_0} \Gamma_p\left(\frac{1-p}{4}\right)^{-1}, \\ \left(\frac{p-1}{2}\right)! &= \Gamma_p\left(\frac{1-p}{2}\right)^{-1}, \quad (\text{ただし } (a)_n = a(a+1)\cdots(a+n-1)) \end{aligned}$$

となり, 従って

$$H_{a,b} = a^{\frac{p-1}{4}} \frac{\Gamma_p\left(\frac{1-p}{4}\right)^2}{\Gamma_p\left(\frac{1-p}{2}\right)} \sum_{i_0=0}^{\frac{p-5}{12}} \frac{\left(\frac{1-p}{12}\right)_{i_0} \left(\frac{5-p}{12}\right)_{i_0} \left(\frac{9-p}{12}\right)_{i_0}}{\left(\frac{3+p}{4}\right)_{i_0} \left(\frac{1}{2}\right)_{i_0} i_0!} \left(-\frac{27b^2}{4a^3}\right)^{i_0}$$

となる. $b \neq 0$ のときは k_0 を用いてまとめる. 他の場合も同様である. ここで $p \equiv a' \pmod{12}$ ($a' = 1, 5, 7, 11$) のとき超幾何多項式 ${}_3\tilde{F}_2$ を

$${}_3\tilde{F}_2 \left(\begin{matrix} a_0 & a_1 & a_2 \\ b_1 & b_2 \end{matrix} \middle| x \right) = \sum_{m=0}^{\frac{p-a'}{12}} \frac{(a_0)_m (a_1)_m (a_2)_m}{m! (b_1)_m (b_2)_m} x^m$$

で定義すれば $H_{a,b}$ は次で与えられる.

定理 2.

(i) $a \neq 0$ のとき

$$H_{a,b} = \begin{cases} a^{\frac{p-1}{4}} \frac{\Gamma_p\left(\frac{1-p}{4}\right)^2}{\Gamma_p\left(\frac{1-p}{2}\right)} {}_3\tilde{F}_2 \left(\begin{matrix} \frac{1-p}{12} & \frac{5-p}{12} & \frac{9-p}{12} \\ \frac{3+p}{4} & \frac{1}{2} \end{matrix} \middle| -\frac{27b^2}{4a^3} \right) & p \equiv 1, 5 \pmod{12}, \\ a^{\frac{p-7}{4}} b \frac{\Gamma_p\left(\frac{-1-p}{4}\right) \Gamma_p\left(\frac{7-p}{4}\right)}{\Gamma_p\left(\frac{1-p}{2}\right)} {}_3\tilde{F}_2 \left(\begin{matrix} \frac{7-p}{12} & \frac{11-p}{12} & \frac{15-p}{12} \\ \frac{p+5}{4} & \frac{3}{2} \end{matrix} \middle| -\frac{27b^2}{4a^3} \right) & p \equiv 7, 11 \pmod{12}. \end{cases}$$

(ii) $b \neq 0$ のとき

$$H_{a,b} = \begin{cases} b^{\frac{p-1}{6}} \frac{\Gamma_p\left(\frac{1-p}{3}\right) \Gamma_p\left(\frac{1-p}{6}\right)}{\Gamma_p\left(\frac{1-p}{2}\right)} {}_3\tilde{F}_2 \left(\begin{matrix} \frac{1-p}{3} & \frac{1-p}{12} & \frac{7-p}{12} \\ \frac{1}{3} & \frac{2}{3} \end{matrix} \middle| -\frac{4a^3}{27b^2} \right) & p \equiv 1, 7 \pmod{12}, \\ ab^{\frac{p-5}{6}} \frac{\Gamma_p\left(\frac{2-p}{3}\right) \Gamma_p\left(\frac{5-p}{6}\right)}{\Gamma_p\left(\frac{1-p}{2}\right)} {}_3\tilde{F}_2 \left(\begin{matrix} \frac{5-p}{12} & \frac{11-p}{12} & \frac{2-p}{3} \\ \frac{2}{3} & \frac{4}{3} \end{matrix} \middle| -\frac{4a^3}{27b^2} \right) & p \equiv 5, 11 \pmod{12}. \end{cases}$$

更に $H_{a,b}$ を有限体上の超幾何級数を用いて表す.

$p \equiv 5 \pmod{12}$, $a \not\equiv 0 \pmod{p}$ のとき

$${}_3\tilde{F}_2 \left(\begin{matrix} \frac{1-p}{12} & \frac{5-p}{12} & \frac{9-p}{12} \\ \frac{3+p}{4} & \frac{1}{2} \end{matrix} \middle| -\frac{27b^2}{4a^3} \right) \equiv {}_2\tilde{F}_1 \left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ \frac{1}{2} \end{matrix} \middle| -\frac{27b^2}{4a^3} \right) \pmod{p}.$$

$$\text{ただし } {}_2\tilde{F}_1 \left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ \frac{1}{2} \end{matrix} \middle| -\frac{27b^2}{4a^3} \right) = \sum_{i_0=0}^{\frac{p-5}{12}} \frac{\left(\frac{1}{12}\right)_{i_0} \left(\frac{5}{12}\right)_{i_0}}{\left(\frac{1}{2}\right)_{i_0} i_0!} \left(-\frac{27b^2}{4a^3}\right)^{i_0}.$$

更に $\frac{(m)_n}{n!} = (-1)^n \binom{-m}{n}$ 及び $\binom{l}{n} \binom{m}{n}^{-1} = \binom{m}{l}^{-1} \binom{m-n}{l-n}$ (l, m : 有理整数) を使って

$${}_2\tilde{F}_1 \left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ \frac{1}{2} \end{matrix} \middle| -\frac{27b^2}{4a^3} \right) \equiv \left(\frac{p-1}{12}\right)^{-1} \sum_{i_0=1}^{\frac{p-5}{12}} (-1)^{i_0} \binom{\frac{5p-1}{12}}{i_0} \binom{\frac{p-1}{2} - i_0}{\frac{p-5}{12} - i_0} \left(-\frac{27b^2}{4a^3}\right)^{i_0} \pmod{p}.$$

一般に $p \equiv a' \pmod{12}$ のとき $P(A; B, C|X) := \sum_{i_0=0}^{\frac{p-a'}{12}} (-1)^{i_0} \binom{A}{i_0} \binom{B-i_0}{C-i_0} X^{i_0}$ とおくと

$$H_{a,b} \equiv a^{\frac{p-1}{4}} \left(\frac{p-1}{2}\right) \left(\frac{p-1}{12}\right)^{-1} P\left(\frac{5p-1}{12}; \frac{p-1}{2}, \frac{p-5}{12} \middle| -\frac{27b^2}{4a^3}\right) \pmod{p}$$

となる. 更に

$$\left(\frac{p-1}{2}\right) \left(\frac{p-1}{12}\right)^{-1} \equiv \frac{\Gamma_p\left(\frac{1}{4}\right)^2}{\Gamma_p\left(\frac{1}{12}\right) \Gamma_p\left(\frac{5}{12}\right)} \pmod{p}$$

であるが, Γ_p の distribution relation により

$$\frac{\Gamma_p\left(\frac{1}{12}\right) \Gamma_p\left(\frac{5}{12}\right)}{\Gamma_p\left(\frac{1}{4}\right)^2} \equiv -(-3)^{\frac{p-1}{4}} \pmod{p},$$

を得る. 一方

$$P(A; B, C|x) \equiv (-1)^{B+C} \sum_{i_0=0}^{p-2} \binom{\omega^{-A}\omega^{i_0}}{\omega^{i_0}}^* \binom{\omega^{-C}\omega^{i_0}}{\omega^{-B}\omega^{i_0}}^* \omega^{i_0}(x) \pmod{p}.$$

であることから 有限体上の超幾何級数

$${}_2F_1 \left(\begin{matrix} \omega^{-A} & \omega^{-B} \\ \omega^{-C} \end{matrix} \middle| x \right) = \frac{p-1}{p} \sum_{i_0=0}^{p-2} \binom{\omega^{-A+i_0}}{\omega^{i_0}}^* \binom{\omega^{-C+i_0}}{\omega^{-B+i_0}}^* \omega^{i_0}(x),$$

を用いれば 他の場合も同様にして次を得る.

定理 3. $j = 3^3 4^3 \frac{4a^3}{4a^3 + 27b^2}$ は絶対不変量である.

(i) $j \neq 0$ のとき

$$H_{a,b} \equiv \begin{cases} -\left(\frac{a}{3}\right)^{\frac{p-1}{4}} p_2 F_1 \left(\begin{matrix} \omega^{-\frac{p-1}{12}} & \omega^{-\frac{5(p-1)}{12}} \\ & \omega^{-\frac{p-1}{2}} \end{matrix} \middle| 1 - \frac{3^3 4^3}{j} \right) (\bmod p) & p \equiv 1 (\bmod 12), \\ -\left(\frac{a}{3}\right)^{\frac{p-1}{4}} p_2 F_1 \left(\begin{matrix} \omega^{-\frac{5p-1}{12}} & \omega^{-\frac{p-5}{12}} \\ & \omega^{-\frac{p-1}{2}} \end{matrix} \middle| 1 - \frac{3^3 4^3}{j} \right) (\bmod p) & p \equiv 5 (\bmod 12), \\ \frac{b}{2} \left(\frac{a}{3}\right)^{\frac{p-7}{4}} p_2 F_1 \left(\begin{matrix} \omega^{-\frac{p-7}{12}} & \omega^{-\frac{5p-11}{12}} \\ & \omega^{-\frac{p-3}{2}} \end{matrix} \middle| 1 - \frac{3^3 4^3}{j} \right) (\bmod p) & p \equiv 7 (\bmod 12), \\ \frac{b}{2} \left(\frac{a}{3}\right)^{\frac{p-7}{4}} p_2 F_1 \left(\begin{matrix} \omega^{-\frac{5p-7}{12}} & \omega^{-\frac{p-11}{12}} \\ & \omega^{-\frac{p-3}{2}} \end{matrix} \middle| 1 - \frac{3^3 4^3}{j} \right) (\bmod p) & p \equiv 11 (\bmod 12). \end{cases}$$

(ii) $j \neq 3^3 4^3$ のとき

$$H_{a,b} \equiv \begin{cases} (-1)^{\frac{p-1}{12}+1} \left(\frac{b}{2}\right)^{\frac{p-1}{6}} p_2 F_1 \left(\begin{matrix} \omega^{-\frac{p-1}{12}} & \omega^{-\frac{7(p-1)}{12}} \\ & \omega^{-\frac{2(p-1)}{3}} \end{matrix} \middle| \frac{j}{j-3^3 4^3} \right) (\bmod p) & p \equiv 1 (\bmod 12), \\ (-1)^{\frac{p-5}{12}+1} \frac{a}{3} \left(\frac{b}{2}\right)^{\frac{p-5}{6}} p_2 F_1 \left(\begin{matrix} \omega^{-\frac{p-5}{12}} & \omega^{-\frac{7p-11}{12}} \\ & \omega^{-\frac{2(p-1)}{3}} \end{matrix} \middle| \frac{j}{j-3^3 4^3} \right) (\bmod p) & p \equiv 5 (\bmod 12), \\ (-1)^{\frac{p-7}{12}} \left(\frac{b}{2}\right)^{\frac{p-1}{6}} p_2 F_1 \left(\begin{matrix} \omega^{-\frac{7p-1}{12}} & \omega^{-\frac{p-7}{12}} \\ & \omega^{-\frac{2(p-1)}{3}} \end{matrix} \middle| \frac{j}{j-3^3 4^3} \right) (\bmod p) & p \equiv 7 (\bmod 12), \\ (-1)^{\frac{p-11}{12}} \frac{a}{3} \left(\frac{b}{2}\right)^{\frac{p-5}{6}} p_2 F_1 \left(\begin{matrix} \omega^{-\frac{7p-5}{12}} & \omega^{-\frac{p-11}{12}} \\ & \omega^{-\frac{2(p-1)}{3}} \end{matrix} \middle| \frac{j}{j-3^3 4^3} \right) (\bmod p) & p \equiv 11 (\bmod 12). \end{cases}$$

参考文献

- [1] S.CHOWLA, B.DWORK and R.EVANS, *On the mod p^2 determination of $\left(\frac{p-1}{4}\right)$* , J. Number Theory, **24**(1986), 188-196.
- [2] M.DEURING, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Univ. Hamburg, **14**(1941), 197-272.
- [3] M.ISHIBASHI, H.SATO, K.SHIRATANI, *On the Hasse invariants of elliptic curves*, Kyushu J. of Math., **48**(1994), 307-321.
- [4] M.KANEKO, *Supersingular elliptic curves and hypergeometric series (in Japanese)*, R.I.M.S., **844**(1993), 17-25.

- [5] M.KANEKO and D.ZAGIER, *Supersingular j -invariants, hypergeometric series, and Atkin's orthogonal polynomials*, to appear.
- [6] M.KOIKE, *Hypergeometric series over finite fields and Apéry numbers*, Hiroshima Math. J., **22**(1992), 461-467.
- [7] M.KOIKE, *Shift orthogonal matrices obtained from hypergeometric series over finite fields and elliptic curves over finite fields*, to appear in Hiroshima Math. J..